

1 The opinion in support of the decision being entered today is *not* binding
2 precedent of the Board
3

4 UNITED STATES PATENT AND TRADEMARK OFFICE
5

6
7 BEFORE THE BOARD OF PATENT APPEALS
8 AND INTERFERENCES
9

10
11 *Ex parte* RICHARD PAUL TARQUINI, RICHARD LOUIS SCHERTZ,
12 and CRAIG ANDERSON
13

14
15 Appeal 2007-0477
16 Application 10/003,510
17 Technology Center 2100
18

19
20 Decided: July 17, 2007
21

22
23 *Before* JAMES D. THOMAS, ALLEN R. MACDONALD, and JAY P.
24 LUCAS, *Administrative Patent Judges*.
25

26 MACDONALD, *Administrative Patent Judge*.
27
28
29
30
31

32 DECISION ON APPEAL
33
34
35
36
37

38 AFFIRMED

STATEMENT OF CASE

Appellants appeal under 35 U.S.C. § 134 from a Final Rejection of claims 1 to 16. We have jurisdiction under 35 U.S.C. § 6(b).

Appellants invented a method and computer readable medium for integrating a decode engine with an intrusion detection system. (Specification 1).

Independent claims 1 and 10 under appeal reads as follows:

1. A method of detecting network-intrusions at a first node of a network, comprising:

identifying a frame as an intrusion by an intrusion detection application;

archiving event-data associated with the frame; and

decoding the event-data by a decode engine, the decode engine integrated within the intrusion detection application.

10. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

identifying, by an intrusion detection application, a frame of data as intrusion- related; and

decoding, by the intrusion detection application, the intrusion-related data.

1 The prior art relied upon by the Examiner in rejecting the claims on
2 appeal is:

3	Trcka	US 6,453,345 B2	Sep. 17, 2002
4			(filed May 7, 1997)
5	Porras	US 6,704,874 B1	Mar. 9, 2004
6			(filed Jul. 25, 2000)

7
8 The Examiner rejected claim 10 under 35 U.S.C. § 102(e) as being
9 anticipated by Porras.

10 The Examiner rejected claims 1-9 and 11-16 under 35 U.S.C. § 103(a)
11 as being unpatentable over Porras and Trcka.

12 Appellants contend that the claimed subject matter is not anticipated
13 and would not have been obvious. More specifically, Appellants contend:

14 1) As to claims 1-9, that the Examiner relies on the monitoring
15 system 22 of Porras as corresponding to the “intrusion detection
16 application,” but the Examiner offers no support or showing that
17 Porras’s translation module 32 (decode engine) is “integrated within”
18 system 22 as required by claim 1. (Br. 6).

19 2) As to claim 10, that the Examiner again relies on the
20 monitoring system 22 of Porras as corresponding to the “intrusion
21 detection application,” but offers no support or showing that Porras’s
22 system 22 “decod[es] . . . the intrusion-related data” as required by
23 claim 10. Further, module 32 performs this function and module 32 is
24 not part of system 22 of Porras. (Br. 8).

25 3) As to claims 11-16 which depend from claim 10, Trcka does
26 not remedy the defects of Porras. (Br. 8).

The Examiner contends monitoring system 22 and translation module 32 are integrated in network based alert management system 10 of Porras. (Answer 8:20-9:9).

We affirm.

ISSUE

Have Appellants shown that the Examiner has failed to establish that Porras describes “an intrusion detection application” having both “identifying” and “decoding” as required by claims 1 and 10?

FINDINGS OF FACT

Appellants invented a method and computer readable medium for integrating a decode engine with an intrusion detection system. (Specification 1, ll. 7-9).

Porras describes a network-based alert management system 10 (i.e., an intrusion detection application) meeting all the limitations of claim 10 and all the limitations of claim 1 except “archiving” (col. 3, l. 16 to col. 4, l. 25).

Porras describes that system 10 includes fault monitoring systems 22 for identifying intrusions (col. 3, ll. 30-37, and col. 3, l. 54 to col. 4, l. 1).

Porras describes that system 10 includes translation module 32 (i.e., decoding engine) (col. 3, ll. 30-37, and col. 3, l. 54 to col. 4, l. 1).

Trcka describes using archival data in a network security system (col. 11, ll. 27-48).

PRINCIPLES OF LAW

On appeal, Appellants bear the burden of showing that the Examiner has not established a legally sufficient basis for anticipation based on the Porras patent.

Appellants may sustain this burden by showing that the prior art reference relied upon by the Examiner fails to disclose an element of the claim. It is axiomatic that anticipation of a claim under § 102 can be found only if the prior art reference discloses every element of the claim. *See In re King*, 801 F.2d 1324, 1326, 231 USPQ 136, 138 (Fed. Cir. 1986) and *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1458, 221 USPQ 481, 485 (Fed. Cir. 1984).

On appeal, Appellants bear the burden of showing that the Examiner has not established a legally sufficient basis for combining the teachings of Porras with those of Trcka.

“Section 103 forbids issuance of a patent when ‘the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.’” *KSR Int’l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734, 82 USPQ2d 1385, 1391 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966). *See also KSR*, 127 S. Ct. at

1 1734, 82 USPQ2d at 1391 (“While the sequence of these questions might be
2 reordered in any particular case, the [*Graham*] factors continue to define the
3 inquiry that controls.”)

4 In *KSR*, the Supreme Court emphasized “the need for caution in
5 granting a patent based on the combination of elements found in the prior
6 art,” *id.* at 1739, 82 USPQ2d at 1395, and discussed circumstances in which
7 a patent might be determined to be obvious without an explicit application of
8 the teaching, suggestion, motivation test.

9 In particular, the Supreme Court emphasized that “the principles laid
10 down in *Graham* reaffirmed the ‘functional approach’ of *Hotchkiss*, 11
11 How. 248.” *KSR* at 11 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12
12 (1966) (emphasis added)), and reaffirmed principles based on its precedent
13 that “[t]he combination of familiar elements according to known methods is
14 likely to be obvious when it does no more than yield predictable results.” *Id.*
15 The Court explained:

16 When a work is available in one field of endeavor,
17 design incentives and other market forces can
18 prompt variations of it, either in the same field or a
19 different one. If a person of ordinary skill can
20 implement a predictable variation, §103 likely bars
21 its patentability. For the same reason, if a
22 technique has been used to improve one device,
23 and a person of ordinary skill in the art would
24 recognize that it would improve similar devices in
25 the same way, using the technique is obvious
26 unless its actual application is beyond his or her
27 skill.

1 *Id.* at 1740, 82 USPQ2d at 1396. The operative question in this “functional
2 approach” is thus “whether the improvement is more than the predictable use
3 of prior art elements according to their established functions.” *Id.*

4 Under this framework, once an Examiner demonstrates that the
5 elements are known in the prior art and that one of ordinary skill could
6 combine the elements as claimed by known methods and would recognize
7 that the capabilities or functions of the combination are predictable, then the
8 Examiner has made a prima facie case that the claimed subject matter is
9 likely to be obvious. The burden then shifts to the Appellant to show that
10 the Examiner erred in these findings or to provide other evidence to show
11 that the claimed subject matter would have been nonobvious.

12
13 ANALYSIS

14 As to claim 10, the Examiner correctly shows where all the claimed
15 features appear in the Porras prior art reference. (See Findings of Fact
16 above.).

17 As to claim 1, the Examiner correctly shows where all the claimed
18 features except “archiving” appear in the Porras prior art reference.

19 As we have already found, Porras explicitly describes that system 10
20 includes systems 22 and module 32. Thus, contrary to Appellants’
21 contentions, Porras teaches a decode engine integrated within an intrusion
22 detection application. Appellants have not established that the Examiner
23 erred with respect to this contention.

1 Appellants arguments appear to be based on an erroneous reading of
2 the Examiner's rejections (e.g., Answer 4:11-20). The Examiner's rejection
3 of claim 1 reads in part:

4 Regarding Claim 1 Porras teaches a method of detecting
5 network-intrusions [detecting suspicious activities, such as intrusion,
6 and based on that generating digital alerts] (Fig. 1 Item 22, and col. 1
7 line 26 to line 28) at a first node of a network [Fig. 1, item 12],
8 comprising:
9 identifying [sensors 22 monitoring various host/network traffic
10 for suspicious activities] frame [streams] as an intrusion by an
11 intrusion detection application (col. 3 line 30 to line 37, and col. 3
12 line 54 to col. 4 line 1);
13 archiving event-data [raw, unprocessed alerts] associated with
14 the frame [streams]; and
15 decoding [translation module 32] the event-data by a decode
16 engine [aggregation, that is combining alerts produced by a single
17 monitoring sensor] (col. 6 line 2 to line 5), the decode engine
18 integrated within the intrusion detection application (col. 4 line 1 to
19 line 25).

20
21 Appellants interpret the Examiner's citation at the end of the
22 "identifying" step as referring to only the immediately preceding "intrusion
23 detection application," rather than the entire preceding "identifying" step.
24 Appellants are in error as is shown by the Examiner's citation at the end of
25 the "decoding" step above. The Examiner's discussions of both steps above
26 are similarly structured in that they conclude with a citation preceded by
27 "intrusion detection application." Appellants' interpretation of the first
28 citation (identifying step) as referring solely to the "intrusion detection
29 application" fails to acknowledge and give a reasonable meaning to the
30 second citation (decoding step).

CONCLUSIONS OF LAW

(1) Appellants have failed to establish that the Examiner erred in rejecting claim 10 as being unpatentable under 35 U.S.C. § 102(e) over Porras.

(2) Appellants have failed to establish that the Examiner erred in rejecting claims 1-9 and 11-16 as being unpatentable under 35 U.S.C. § 103(a) over Porras and Trcka.

(3) Claims 1-16 are not patentable.

DECISION

The Examiner's rejection of claims 1-16 is Affirmed.

AFFIRMED

rwk

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins CO 80527-2400